takebackthetech

GUIDE TO Protecting Yourself From Digital Stalking

Rohini Lakshané

Take Back The Tech!
(2024)

Guide to Protecting Yourself from Digital Stalking

Rohini Lakshané

Take Back The Tech! (2024)

Guide to Protecting Yourself from Digital Stalking by Rohini Lakshané/ Take Back The Tech! is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) License, except where otherwise noted. More licensing information at https://www.takebackthetech.net/index.php/copyleft

This e-book contains a four-part guide in English, which was later translated to French and Spanish.

First published at Take Back The Tech! in 2024—
https://www.takebackthetech.net/

Illustrations by Laura Ibáñez López.
https://cargocollective.com/pakitalouter

Cover design by Arvind Joshi

This book was designed by Arvind Joshi with *Canva*
The image on the cover page is taken from *Envato*

About the author

Rohini Lakshané is an award-winning interdisciplinary researcher, technologist, and Wikimedian. Technology-facilitated gender-based violence (TFGBV) is a major area of her work. An engineer by training, Rohini has worked on several research and advocacy projects at the intersection of technology, policy, and civil liberties. Full bio at https://about.me/rohini

About the publisher

Take Back The Tech! is a call to everyone, especially women and girls, to take control of technology to end violence against women. It's a global, collaborative campaign project that highlights the problem of tech-related violence against women, together with research and solutions from different parts of the world. Take Back The Tech! was initiated in 2006 by the Association for Progressive Communications (APC) Women's Rights Programme and has grown into a diverse movement of individuals, organisations, collectives and communities. More information at https://www.takebackthetech.net/node/1

About this e-book

This e-book contains a four-part guide on the topic of tech-facilitated stalking, especially perpetrated by current or former intimate partners. This guide is intended for victim-survivors in global majority countries. For queries and collaboration requests, email the author at first name dot last name at gmail dot com.

Contents

1. Protecting against stalkerware and exposure of private images
2. Tech-facilitated intimate partner stalking countermeasures: Part 1
3. Tech-facilitated intimate partner stalking countermeasures: Part 2
4. Tech-facilitated intimate partner stalking countermeasures: Part 3

Protecting against stalkerware and exposure of private images

Rohini Lakshané

Search for “How to spy on my spouse” on the internet (or replace “spouse” with “lover”, “girlfriend”, or “boyfriend”) and it reveals a disturbing reality. There are scores of results for persons who suspect their partners of infidelity, or are frustrated and

heart-broken over an unexpected or messy break-up, or facing separation, divorce, or a child custody battle. The results demonstrate what happens when the surveillance economy meets abusive intimate partners. There is a variety of advice including suggestions to hire a private detective who provides information and evidence of the target's activities, to install tiny spy cameras in the places where the target expects privacy, or to stalk them via their laptop or phone.

Imagine a scenario where someone convinces their partner to install a 'safety app' to know their location in case of emergencies. The app is supposed to pick up and convey the device's location only when its user triggers an SOS alert, which it sends to their emergency contact(s), in this case, the partner. Such location tracking can sound as if it comes from a place of concern. Yet, in reality and frequently unbeknownst to the partner, the app also allows constant monitoring of their movements. Such an app is an example of stalkerware, a term for a set of tools -- software programs, apps or devices[1] -- that enables secret surveillance, often used by employers, abusive intimate partners or exes. The term "spouseware" is sometimes used to refer specifically to stalkerware deployed by spouses.

Stalkerware in disguise

Stalkerware can masquerade as legitimate and useful software. To quote another example, two schools in

Philadelphia installed the LANrev TheftTrack program on the laptops it issued to students. A feature in the programme meant to track stolen or misplaced laptops allowed administrators to remotely and clandestinely switch on the laptop's camera. In 2010, it was discovered that some students were photographed without their knowledge on laptops that were not reported as missing or stolen. Some of the photos allegedly showed them nude or partially nude in their homes.

Some stalkerware are programmed to automatically hide themselves when installed on devices. They lack an icon and mimic legitimate processes in the phone's software to evade detection.

Kaspersky's annual The State of The Stalkerware report identifies the top 10 stalkerware apps in the world in terms of the number of affected users: TrackView, Reptilic, SpyPhone, MobileTracker, Cerberus, Wspy, Unisafe, Mspy, MonitorMinor, and KeyLog. While the number of affected users in the 2023 report ranges from approximately 800 to 4,000, the actual incidence of stalkerware apps is likely to be higher.

The invasiveness of stalkerware

Installing stalkerware typically requires physical access to the target's device, but the technical know-how needed is minimal. Alarmingly, a plethora of commercially available

apps marketed for parental control or employee monitoring can be easily repurposed for stalking, making them a tool of abuse, coercion and harassment. Take for instance, KidsGuard Pro, sold by its developer ClevGuard as a parental control app. It offers a range of functionalities, including allowing the stalker to remotely:

- View call history, texts (even deleted ones), and record phone calls
- Take screenshots and a video recording of the screen
- Activate the camera and microphone to capture photos, videos and audio of the surroundings
- Track GPS location and view location history
- Read messages on instant messaging and social media apps
- View browsing history
- Access photos, videos, documents, calendars and other files

All of this happens without the target's knowledge. This level of detail makes the stalker privy to every aspect of the target's life. The stalker can view, for example, a doctor's appointment on the calendar, a copy of an ID stored in the files, a credit card statement revealing a security purchase such as a video phone for the door, chats with a new match on a dating app (and thus the prospect of a new partner), or a recording of a phone call the target made to a friend

describing the stalker's domestic abuse. ClevGuard indeed lists it among the "best spy apps" to "determine if your spouse is cheating."

Intimate partner abuse is seldom restricted to either the online or the offline realm; it is pervasive. If an intimate partnStalkerware stalkerware, chances are high that the person being surveilled is already experiencing abuse, violence, coercive control, or harassment in the relationship or even after the relationship has ended. The detailed information it gathers allows the stalker to know when and where their target is likely to be vulnerable, or even impede their attempts to escape or seek help. This can lead to further abuse, a threat to the target's safety, and may overall exacerbate the situation.

How stalkerware leads to image-based abuse

One of the potential threats of stalkerware is image-based abuse. Colloquially called "revenge porn", image-based abuse occurs when someone captures, creates, publishes, distributes or threatens to distribute the nude or sexually explicit images or videos of another person without their consent. Such images and videos are called "non-consensual intimate images" (NCII). These are modes via which stalkerware may lead to image-based abuse:

Remote capture: Stalkerware can be used to remotely switch on the phone's camera and microphone to clandestinely

shoot photos and videos when the target is nude or in a sexual act. The stalker may distribute or threaten to distribute this content.

Exploiting existing images: The stalker can also access nude selfies and sexually explicit videos that are already stored on the device, giving them ammunition for future threats or distribution.

Accidental leaks: Even if the stalker does not intend to share the images, leaks can happen due to, say, lost or stolen phones, compromised media-storage accounts in the cloud, or email hacking.

Once put into circulation on the internet, the images are extremely hard to remove completely. Those removed from one location on the internet may reappear elsewhere. This is known as downstream distribution.

Image-based abuse has a devastating impact on all aspects of the lives of victim-survivors who face public humiliation, stigma, social boycott, job loss, abandonment by family, and mental and physical health issues, and many more ramifications. Some consider suicide. (For more information about the impact on victim-survivors, the modessextortione, access, and distribution of images and videos, and remedies, refer to the paper, Non-consensual intimate imagery: an overview.)

The stalker or anyone else who comes to be in possession of these images may resort to "sextortion". They may extort money from the target, or demand more sexual imagery or favours in return for not distributing the images on the internet or not sending the images to specific persons known to the victims.

The stalker may also use the images to intimidate or manipulate the target. A former lover may demand getting back in the relationship. A separated spouse may lay down coercive conditions in divorce, alimony or child custody proceedings.

Data insecurity

The security of stalkerware is concerning. Several investigations conducted by researchers and journalists over the years (see here, here, and here) have found that various stalkerware leaked data and suffered data breaches at the hands of unethical hackers, affecting hundreds of thousands of their users and the targets the users were surveilling.

Leaked data often ends up on the public internet (and the dark web), and may contain the NCII of the targets along with their personally-identifying information such as names, locations, and social media profiles. It is thus a gold mine for cybercriminals. It puts the victims at the risk of several kinds of harm including image-based abuse, identity theft, and extortion. The images and infsextortionbtained from the

leaked dumps on the internet can be reposted elsewhere. Extortion and defamation websites such as the now-defunct IsAnyoneUp display intimate images with personal information and demand money for their removal, which is an act of sextortion.

The problem with the security of stalkerware is three-fold:

- Stalkerware companies prioritise profit over the security of their software and sensitive data. This lack of responsibility is unsurprising. Companies that profit from interpersonal trust issues and unethical (and potentially illegal) surveillance are unlikely to invest in robust security measures. As Eva Galperin, Director of Cybersecurity at the Electronic Frontier Foundation, puts it, "The people who run these companies are perhaps not the most scrupulous or really concerned about the quality of their product."
- Stalkerware is an attractive target for malicious hackers because of the volume and sensitive nature of the data it collects and holds, and its relatively lax security measures.
- As long as the stalkerware exists on the internet, data leaked to harmful entities is a constant threat to the stalkerware's targets, putting them at further risk of cybercrime and exploitation.

Addressing image-based abuse via stalkerware

The cheapest and simplest safeguard against the surreptitious capture of photos and videos via stalkerware and other kinds of spyware is to use removable stickers that physically cover the camera lens. These go by the names "camera covers", "privacy stickers" etc. It is advisable to either switch off the phone or keep it away (inside a backpack or a similar enclosed space), during intimate acts and sensitive conversations because stalkerware may record the events in its surroundings. Some more strategies and resources for victim-survivors are stated in the previously mentioned paper.

Cleaning up sensitive data and protecting it with encryption helps. However, some kinds of stalkerware can access the contents of even encrypted messaging apps and file storage.

Detecting and removing stalkerware

Note: Searching for stalkerware, removing or disabling it may alert the stalker and may potentially cause the abuse to escalate. Please use your discretion while following the suggestions in this article, and have a safety plan. It is advisable to seek specialised support for this, using a device and a connection that the stalker does not use and is not likely to surveil.

The Coalition Against Stalkerware offers a wealth of information about stalkerware, getting help, and resources for survivors through StopStalkerware.org. This includes information about local support groups in some parts of the world.

The DeStalk campaign offers information and resources for survivors and those supporting them, and a free e-learning course on cyberviolence and stalkerware. It is located in Europe, so the advice and resources are mostly Europe-centric.

Anti-malware software such as those developed by Kaspersky and MalwareBytes flags the stalkerware it finds on a device. These software are available for a variety of operating systems and types of devices. A precaution is to avoid malicious apps posing as well-known software for enhancing security and privacy. Malicious software (called "malware") can masquerade as anti-malware. For information about identifying fake apps and software, refer to this and this article.

Kaspersky has also developed a free tool called TinyCheck, which allows users to discreetly check whether spyware is installed on their devices. However, using it may require some degree of technical knowledge. This article provides more information about TinyCheck, how to use it, and stalkerware in the context of intimate partner abuse.

TechCrunch offers this spyware lookup tool and instructions to check whether an Android device was compromised by TheTruthSpy stalkware app or other apps in its cluster. These apps belong to a network of commercially available stalkerware.

The Safety Net project offers a guide for checking devices for rooting and jailbreaking as a part of a larger toolkit for victim-survivors of violence. Rooting and jailbreaking enables abusive partners to compromise the security of devices in many ways, making them more vulnerable to stalkerware and other threats.

In terms of preventive measures,

- Be cautious about app downloads: Only install apps from trusted sources.
- Keep software updated: Regularly update your operating system, apps and security software.
- Be mindful of public Wi-Fi: Avoid accessing sensitive information on unsecured networks.
-

Recommended viewing: The Myths and Realities of Stalkerware video by Safety Net Project.

The next part in this series explores countermeasures for popular techniques used by stalkers that involve commonly used apps, features and online services.

1 Definition adapted from the Coalition Against Stalkerware https://stopstalkerware.org/

First published at https://www.takebackthetech.net/blog/protecting-against-stalkerware-and-exposure-private-images on 5 November 2024.

DOI: https://doi.org/10.5281/zenodo.14172568

Translation/ Traduction/ Traducción

Français:
https://www.takebackthetech.net/fr/blog/se-proteger-contre-le-stalkerware-et-la-diffusion-dimages-intimes

Español:
https://www.takebackthetech.net/es/blog/proteccion-contra-el-stalkerware-y-la-exposicion-de-imagenes-privadas

ROHINI LAKSHANÉ

Tech-facilitated intimate partner stalking countermeasures: Part 1

Rohini Lakshané

Note: *Searching for, removing or disabling the means of stalking may alert the stalker. This may potentially cause the abuse to escalate, pose a risk to the target's physical safety, and close their avenues to seek help or exit the relationship. If you are someone experiencing stalking or supporting someone who is, please assess*

the situation first. It is advisable to seek specialised support, using a device and a connection that the stalker does not use and is not likely to surveil. Please use your discretion while following the suggestions in this article, and have a safety plan.

The dynamics of intimate partner stalking are complex and often deeply rooted in the shared history between the target and the stalker. A current or former intimate partner is often privy to information about one's past experiences, life history, daily routine, habits, aspirations, future plans, personal anxieties, vulnerabilities, and more. The intimate partner may have a good amount of knowledge of one's personality traits, patterns of behaviour, typical responses in different situations, and so on. A stalker can take advantage of even seemingly harmless or trivial information about the target by triangulating it with this intimate knowledge. This article shines a light on some potential countermeasures against popular techniques of stalking that involve commonly used apps, features, online services and devices.

Securing digital presence and communication

Intimate relationships involve sharing both trivial and sensitive digital information and devices for the sake of routine and convenience – passwords, identity documents or numbers, location, shared accounts, and so on. When a relationship is about to end or has ended, it is crucial to remove the ex-partner's access to this information and to

devices to prevent intentional misuse or accidental exposure. The Digital Breakup Guide by Refuge and Avast contains suggestions to secure the use of apps and online services during and after a relationship breakup, especially if there are concerns about abuse or stalking. It categorises the apps and services on the basis of location-based features, email, social media, finance, entertainment, gaming, wellbeing and fitness, travel, food takeaway and delivery, and dating apps. The Safety Net project offers a Technology Safety and Privacy Toolkit in English and Spanish for victim-survivors, which contains useful guides such as making a technology safety plan. The National Network to End Domestic Violence also offers some more tips on safety.

The Consumer Reports article, "A Digital Guide to Breaking Up: How to Reclaim Your Online Accounts After a Relationship Ends" offers useful advice to secure online accounts, along with ways of avoiding and reducing unwelcome reminders of the past.

Restricting communication and access

It is important to recognise that completely cutting off contact with the stalker is not always feasible or safe. For example, blocking the stalker might lead to a severe backlash or when co-parenting with the stalker is necessary, maintaining some level of communication is unavoidable. In such cases, suggestions in the above Consumer Reports article to "restrict", "mute" or "hide" the stalker's profile and

updates on social media can be useful for allowing restricted communication and access.

You may want to store all unwanted communication from the stalker – whether through emails, SMS, social media messages, instant messengers etc – as evidence of stalking and abuse. However, receiving and reading these messages can be distressing, especially if they are frequent or arriving at odd hours. Set up filters in your email and messaging apps to sort or redirect messages from the stalker. This allows you to choose when to engage with incoming communications and reduces the immediate emotional impact. Only read the messages when you feel emotionally prepared to do so.

Email filters: Start by creating a new folder in your email account specifically for the stalker's emails. For each email address used by the stalker, create a filter that automatically directs their emails to the designated folder. If the stalker contacts you from a new email address every time (a tactic to evade or slow down legal action or gain plausible deniability), set up additional filters based on specific keywords or phrases they commonly use in the subject line or body of their emails. For instructions about using filters on Gmail, see here and here, see Protonmail, Microsoft Outlook, Thunderbird or refer to the help pages of your email services provider or preferred email client.

Filtering on apps

Signal: Mute a chat on the Signal app and archive it to prevent its notifications from being displayed. To view new messages from the muted and archived chat, navigate to the Archived Chats section within the app. For more instructions, refer to this page.
WhatsApp: Mute chats and access archived conversations in a dedicated folder.
Telegram: Mute notifications and customise alert settings for specific contacts.
Facebook Messenger: Mute conversations and manage filtered messages from unknown senders.
Various apps for SMS, instant messaging and social media platforms may support some ways of filtering messages; you may want to explore those on your preferred apps and platforms.

Bluetooth

One can pair a mobile phone via Bluetooth to a car's music system, for instance, to play music stored on the phone. However, this allows the car's owner/ driver to view other files and messages stored on the phone when its Bluetooth feature is switched on and within the car's range. Unpair Bluetooth from the stalker's devices to prevent misuse of the connection.

Impersonation and doxxing

Stalkers may employ various tactics to harass, threaten and discredit their targets, including posting defamatory content, creating fake online profiles or pages impersonating the target, and posting their personal information or images without consent. Fake social media profiles may be used to manipulate the target and their social circle. This may pose a threat to the target's reputation, safety and privacy. To proactively monitor and protect your online presence, create a set of Google Alerts to receive email notifications for:

- Your full name (with variations in spelling, and past names, if any)
- Your phone number, email address, street address etc
- Use quotation marks for exact phrase matching

If you run a business, organisation etc., it may also be useful to set up alerts for its name. Stalkers may be interested in information about the individuals, events, initiatives and organisations close to their target. For more, refer to an online reputation management guide, such as this one.

Doxxing is the malicious practice of obtaining and publishing someone's personally-identifying information online without their consent, often as a form of harassment or intimidation. This information can include street addresses, email addresses, phone numbers, identification numbers (driving licence, social security number), and so on. Doxxing oneself, called "self-doxxing", is a useful way of proactively searching for such information, in order to

remove or secure it. The New York Times has a detailed guide and explanatory article about self-doxxing and locking down personal information. (The material is aimed at journalists and activists but is useful for victim-survivors of intimate partner stalking also.)To remove your personally-identifying information (phone number, street address etc), or financial or medical information from Google Search results, refer to the steps in this article under "How to remove search engine results about you".

Maps

Stalkers may post privacy-violating images, videos, information or reviews on the pin location of the home, workplace or other places frequented by their targets. View the pin location of those places on Google Maps and other mapping services to look for privacy-violating content. In addition, stalkers may post defamatory content about these places, such as, suggesting in the reviews that certain illegal activities happen there. If you find private or false information, report it to the platform immediately for removal.

For information about blurring your home on Google Maps Street View, refer to this article.
Some shared accounts such as Netflix or gym memberships also include location features. Take a moment to check if location is activated in any apps or if there are any linked devices as a quick safety step, as the Digital Breakup Guide

suggests. The "location" chapter in the guide contains some useful tips about securing maps and other location-based services.

Public records, online databases and archival information

You might find in the course of self-doxxing or through Google Alerts notifications that your private information has appeared on public records maintained by either a government agency or a privately-owned online database. In that case, you can contact the website/ service and request the removal of your private information or your entire profile. Remember that some websites and pages are backed up on the Internet Archive's Wayback Machine. Contact them for removal at the same time as you make a removal request to the source website from where it was archived.

In some cases, especially if there is a data protection entity in your country, the right to be forgotten can be invoked. It is a right to request that personal data be deleted under certain circumstances.

Notification history

Most smartphones have a "notification history" setting. If the stalker has access to your device, physically or remotely, they may be able to view all notifications including those of messages and emails you deleted. This may potentially

reveal the communications you made for seeking help, exiting the relationship, moving to a safe place etc. In such cases, consider disabling notification history altogether or turning off notifications from some contacts (messages and emails) that you need to keep private, so that they do not show in the notification history. Refer to how to enable/disable and view notification history on an Android phone, and how to view and manage notifications on iPhone or iPad.

The next part of this series of articles takes a look at some more commonly used apps and services for intimate partner stalking, stalkerware devices such as spy cameras, and gaslighting as a technique used by stalkers.

First published at https://www.takebackthetech.net/blog/tech-facilitated-intimate-partner-stalking-countermeasures-part-1 on 5 November 2024.

DOI: https://doi.org/10.5281/zenodo.14172612

Translation/ Traduction/ Traducción

Français:

https://www.takebackthetech.net/fr/blog/se-proteger-contre-le-stalkerware-et-la-diffusion-dimages-intimes

Español:

https://www.takebackthetech.net/es/blog/proteccion-contra-el-stalkerware-y-la-exposicion-de-imagenes-privadas

Tech-facilitated intimate partner stalking countermeasures: Part 2

Rohini Lakshané

This is the third article in this series. The previous articles explained stalkerware and how it may lead to image-based abuse, some popular techniques of stalking that involve commonly used apps, features, online services and devices, and potential countermeasures to them.

Note: *Searching for, removing or disabling the means of stalking may alert the stalker. This may potentially cause the abuse to escalate, pose a risk to the target's physical safety, and close their avenues to seek help or exit the relationship. If you are someone experiencing stalking or supporting someone who is, please assess the situation first. It is advisable to seek specialised support, using a device and a connection that the stalker does not use and is not likely to surveil. Please use your discretion while following the suggestions in this article, and have a safety plan.*

Social media scraping

Publicly available information shared by the target or their contacts on social media is often an easy move for a stalker. For instance, the target may publicly seek help for something, RSVP to an event, or the event organiser may announce the target's attendance at a forthcoming event. These seemingly innocuous posts can reveal the target's whereabouts and plans. Moreover, public posts and actions (likes, comments RSVPs etc) can be accessed discreetly without spending much time, money or effort. The information is meant for all to see, so it carries a lower perceived risk of legal repercussions compared with doing activities that involve actively invading the target's privacy or security. This information can be of a detailed nature depending on the platform and the privacy settings of the target and even the target's contacts.

Using automated tools and scripts to harvest information about individuals, organisations, topics, and more from social media platforms is called "social media scraping". A stalker with sufficient knowledge and skills can scrape publicly available information about you or persons, places, events, and things associated with you from social media or elsewhere on the internet. Blocking the stalker's profile on social media sites is unlikely to completely prevent them from scraping. This article about a specific scraping tool demonstrates how it works, and the sources and types of information it collects.

While being discreet about the information shared on social media and applying optimal privacy settings can reduce exposure, it is unfortunately impossible for the target to prevent a stalker from accessing publicly available information. To effectively deter or thwart stalkers from misusing the information they gather, robust legal and social protections are essential. For information about applying the necessary privacy settings, refer to this article on cyberstalking, and the section on locking down personal information in the self-doxxing guide mentioned earlier.

Dating apps

A recent Kaspersky survey reveals that digital stalking is a significant concern for online daters, with nearly a quarter of users experiencing it. While a dating profile is designed to showcase the best version of oneself, it is useful to carefully

consider how a stalker may misuse the information shared on these platforms. In addition, creating a dating profile signals a desire for new companionship, which could lead to a negative reaction from a stalker who is also a current or former intimate partner. Some dating apps allow you to preemptively block other users via their phone numbers. To improve your privacy on dating apps and protect against cyberstalking, refer to this article and this one.

Some location-based dating, friendship or matrimony apps offer a feature that allows users to share profiles they like with friends. For instance, Bumble's "Recommend to a Friend" feature creates a shareable link to the profile. While intended to facilitate connections, this feature can be exploited by stalkers. A friend of a stalker in your area (dating apps show profiles within a radius or region) might come across your profile and share your information via screenshots or the shareable link. According to one study, some dating apps allow stalkers to access users' near-exact location – an accuracy of 2 metres radius on Bumble and Hinge and 111 metres on Grinder. Even if you block the stalker on the app, they can create multiple accounts using different mobile numbers to access your profile information. Accessing and viewing a profile via the shareable link does not require interacting with the profile.

Spy devices

Cameras, microphones, GPS trackers and other spy devices

when installed without the knowledge and consent of the target are forms of stalkerware. They may be planted in places where the target has an expectation of privacy. In homes, cars, or other personal spaces, cameras and mics make the stalker privy to every aspect of their target's life in those spaces. Cameras in bathrooms or bedrooms may enable the stalker to get access to nude or sexually explicit videos of the target. This may lead to image-based abuse. (For more information about stalkerware and image-based abuse, refer to the first article in this series.)

Spy cameras and microphones (also called "bugs") come in a large variety. Some are capable of connecting to the internet and transmitting the video footage. Others may be housed in casings with in-built memory storage that the stalker can later retrieve. (For example, take a look at the sections "spy camera", "live streaming spy camera", "spy voice recorder" and "GPS trackers and transmitters" on this website that sells them.) Spy cameras and mics are meant to be tiny and discreet (with lenses as small as 1 millimetre) and can be implanted in places such as lamp shades, smoke detectors, air filters and hair dryer holders. Depending on local laws, policies and practices, it may be possible for a stalker to procure a spy device without leaving a paper trail.

This article by the anti-virus software company Norton offers useful advice about how to find hidden cameras while this one by the Safeguarding Hub shines a light on domestic abuse and covert surveillance via cameras, devices for

eavesdropping and location tracking, and smart devices.

Air Tags

AirTags are small devices that connect to nearby Apple devices via Bluetooth. Airtags are useful for finding lost items by tracking their location on Apple's Find My network. Unfortunately, AirTags have been misused in numerous cases for stalking (See here and here). In one case, a man allegedly planted as many as seven AirTags on a car used by his then-wife. He also threatened to expose her sexually explicit images and videos that were in his possession if she did not meet his demands. This article describes AirTag stalking and how to protect against it.

Spy devices are designed to evade detection. Hence, detecting spy devices and evading detection are like a cat-and-mouse game. Thus, the responsibility of always staying safe from stalkerware should never be on the victim-survivor. Spy devices and their detection constitute an entire industry. As an individual and someone in an abusive situation, the victim-survivor may not be able to keep up with invasive devices, tactics and their sophistication. More needs to be done to regulate the sale and availability of spy devices. Depending on the jurisdiction of the victim-survivor, the use of spy devices may amount to unlawful surveillance and other offences. However, legal remedies may be harder to access if the stalker is a current or cohabiting partner who plants these devices in their own home or property such as a

car in order to surveil the target.

CCTV

The cohabiting stalker may install a CCTV camera system or other kinds of cameras (nanny cams or Ring camera, for example) for physical security and monitoring of the home, all of which can be misused to surveil the target. They may be able to remotely change the direction in which the camera is pointed, change the zoom settings, or surreptitiously switch it on and record the target when the target is nude, partially nude or in a sexually explicit act – another potential act of image-based abuse as described in the first article in this series.

A stalker may try to access recorded footage or live streams showing the target from camera security systems installed on the property of other people or in public places. Depending on where you are in the world, it may be possible for the stalker to do so without leaving a paper trail and without the backing of a judicial warrant. For example, the intimate partner-stalker may convince a neighbour to let them access the recording on their CCTV camera or bribe a government clerk or a private security guard to give them access.

Gaslighting

Gaslighting is a form of psychological manipulation that

makes the target doubt their own perceptions, experiences or understanding of events. It makes the targets believe that they may be imagining things or over-reacting to, or misunderstanding certain events and incidents. Gaslighting works insidiously, which makes it hard for the target to gather evidence or prove the goings-on to a third party such as law enforcement. These are some ways in which a stalker may be able to gaslight their target:

Information gathered from the sources that the target is unaware of (as mentioned previously stalkwerware, CCTV camera footage etc.), enables the stalker to manipulate the target in ways that creates self-doubt.

Disappearing emails and messages delete themselves after a period of time set by the sender. Some email and messaging services make the "disappearing time-period" clear to all parties involved in the conversation – WhatsApp, Signal, Protonmail, Telegram etc. However, depending on the email service, a sufficiently skilled stalker may send emails that hide their disappearing nature, in order to alter the target's perception of reality.

Smart home devices, such as those in this list, are networked devices in the home that allow remotely controlling appliances and systems such as heating or air-conditioning. While the target is likely to be aware of the presence of the device in their vicinity, they may not know that it can be remotely controlled. These devices can be used

to gaslight the target by changing their settings, turning them on or off unexpectedly, listening to conversations, or monitoring the target's activities.

Constant surveillance, digital or physical or both, can create a sense of being watched, causing the target to doubt their own perceptions of safety and privacy. This may have severe psychological impacts on the target.

The next and final article in the series shines a light on risk assessment for victim-survivors and detecting the misuse of their images.

First published at https://www.takebackthetech.net/blog/tech-facilitated-intimate-partner-stalking-countermeasures-part-2 on 5 November 2024.

DOI: https://doi.org/10.5281/zenodo.14172638

Translation/ Traduction/ Traducción

Français:
https://www.takebackthetech.net/fr/blog/contrer-le-cyberharcelement-au-sein-du-couple-deuxieme-partie

Español:
https://www.takebackthetech.net/es/blog/medidas-tecnologicas-contra-el-acoso-de-la-pareja-parte-2

ROHINI LAKSHANÉ

Tech-facilitated intimate partner stalking countermeasures: Part 3

Rohini Lakshané

This is the fourth and final article in this series.

Risk assessment

All stalkers are not equal. Different stalkers have

different motives and capabilities. Some want to keep their targets in a state of fear and anxiety but do not have the ability or opportunity to directly cause them physical harm. Some want to destroy the target's reputation or relationships. Some have the means to use a variety of tactics against their targets while not damaging their own public reputation. Thus, it is necessary to evaluate the situation and determine precise responses that are tailored to the situation of the specific victim-survivor. Such an evaluation is called a risk assessment. It is used to effectively determine specific risks and threats that a victim-survivor faces in the present and the future and the potential interventions for their safety and wellbeing.

The Stalking and Harassment Assessment and Risk Profile Tool (SHARP) is a free online tool containing 48 questions that the victim-survivor can answer to evaluate the situation. Upon completion, it generates two detailed reports. One report states the impact of stalking on the victim-survivor. The other is a structured risk profile of the victim-survivor. It also contains suggestions for their safety.

The tool was developed in the United States, so some aspects of it may not be applicable outside the country. Its website offers more resources for victim-survivors, such as this template for documenting stalker behaviour and incidents of stalking.

For more information about the SHARP tool, refer to thisFAQ.

Reverse image search

Some stalkers may post their targets' images (photos or videos) on pornographic websites, defamation websites, adult forums, or sub-Reddits dedicated to pooling the images and information of women and gender-diverse persons without their consent. They may post the images in online profiles impersonating the targets, or alongside text intended to publicly discredit the targets or cast aspersions on their morals or character, for example, "She is a <gendered slur/offensive word>" or "She is a serial cheater in her relationships." The intent is to harm the reputation of the victim-survivor and possibly subject them to targeted harassment from other users of the website or forum towards them.

Reverse image search is useful to detect such images. It allows users to search the internet using images and identify where an image appears online and find similar images. This page (Archive URL) lists a range of free and paid reverse image search tools such as Google Image Search, Bing Image Match, TinEye, Yandex Image Search and PimEyes. These services differ to various extents in finding exact or near matches -- one may be able to detect what the other might not.

All the tools listed require the user to upload the image or provide a URL where the image is already present. A word of

caution is that the reverse image search service might store the images uploaded to it for searching. Hence, nude or sexually explicit images should not be used for searching. Images that are already published on the internet such as social media display photos may be used for searching – those are also the images that stalkers are most likely to find and use. Nude and/ or sexually explicit images of the target, if they are posted online, may appear in the search results depending on the tool used and its safety settings.

In addition to the tools listed above, the following browser extensions are useful if many images of the victim-survivor have been compromised and posted on the internet, for example, by hacking a private folder of their photos.

1. Fast Image Search (Google Chrome, Firefox): It enables the user to search results from Google, TinEye, Yandex (in three languages), Baidu, Bing or any combination of those.

2. RevEye Reverse Image Search (Google Chrome): Search images on Google, Bing, Yandex and TinEye. It also allows users to add other search engines to the menu. The extension for the Firefox browser has not been updated since 2022. Hence, its use is not recommended at the time of writing.

Removal of images

Victim-survivors who may want their unwanted images to be removed may report abuse to the website/ service or email a request asking for removal. Whether or not the website will acquiesce and remove the image depends on a number of factors including the content of the images, the website's/ platforms' own terms of service, community standards, policies for privacy and content, and the laws and legal jurisdiction that apply. Removal requests can be made under these categories (indicative list):

1. Privacy violation (especially for non-consensual nude or sexually explicit content posted without the consent of the persons in the images)
2. Copyright infringement (for images shot by the victim-survivor, for example, selfies. If a friend of the victim-survivor has captured those images, then they are the legal copyright owner. They may file an infringement notice to take them down.)
3. Abusive or illegal content (content that is defamatory, abusive, vulgar, harassing etc.)
4. The right to be forgotten in the jurisdictions where it exists

If the source of the image on the internet does not remove it, it may still be possible to request search engines to remove the image from search results. This reduces the discoverability of the image. This online form can be used to

report safety concerns to the search engine Bing and other Microsoft products while Google Search has policies and a process to request removal of personal content. For more information about removal requests to different platforms, refer to guide Removing Sensitive Content from the Internet. Stalkers may conduct searches of the images of their targets to find more images or the information associated with those images. Thus, it is necessary to note the information posted with the search results and consider whether it may possibly be misused, especially in combination with any other information or documents the stalker may possess. Victim-survivors should request removal of that information along with the images. It is likely that these processes may become lengthy and websites and platforms are slow to respond or completely unresponsive. It is essential to keep copies of all communications in this regard.

Conclusion

Although this series has tried to unpack common ways in which stalkers work and countermeasures to address these, victim-survivors should never have to bear the onus of protecting themselves. Technical safeguards and precautions stated in this article are important but often insufficient in cases of serious and sustained intimate partner stalking. Victim-survivors need adequate and timely legal, psychological, technical and safety support and resources. Society, law enforcement, and support systems must work collaboratively to provide a safety net and holistic support that goes beyond individual precautions.

First published at https://www.takebackthetech.net/blog/tech-facilitated-intimate-partner-stalking-countermeasures-part-3 on 21 November 2024.

DOI: https://doi.org/10.5281/zenodo.14561332

Translation/ Traduction/ Traducción

Français:
https://takebackthetech.net/fr/blog/contrer-le-cyberharcelement-au-sein-du-couple-partie-3

Español:
https://takebackthetech.net/es/blog/medidas-tecnologicas-contra-el-acecho-parte-3